

CLAIMS

1. A method for identifying network traffic comprising:
 - receiving pattern matching data;
 - comparing the pattern matching data with a pattern; and
 - 5 determining whether the pattern matching data matches the pattern.
2. A method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes application data.
3. A method for identifying network traffic as recited in Claim 1, in the event that the pattern matching data matches the pattern, further including determining a property
10 associated with the network traffic.
4. A method for identifying network traffic as recited in Claim 1, in the event that the pattern matching data matches the pattern, further including determining a property associated with the network traffic; wherein the property is an application protocol.
5. A method for identifying network traffic as recited in Claim 1, in the event that
15 the data matches the pattern, further including determining a property associated with the data and assigning a score for the property.
6. A method for identifying network traffic as recited in Claim 1, in the event that the data matches the pattern, further including determining a property associated with the data; and applying a policy based on the property.
- 20 7. A method for identifying network traffic as recited in Claim 1, further comprising assigning a score to a match if the pattern matching data matches the pattern.

8. A method for identifying network traffic as recited in Claim 1, further comprising:

assigning a first score to a first match if the pattern matching data matches the pattern;

5 comparing the pattern matching data with a second pattern;

assigning a second score to a second match if the pattern matching data matches a second pattern.

9. A method for identifying network traffic as recited in Claim 8, further comprising determining a property associated with the traffic by comparing the first score and the
10 second score.

10. A method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes a string selected from a packet.

11. A method for identifying network traffic as recited in Claim 1, wherein pattern matching data includes concatenated application data of a plurality of packets.

15 12. A method for identifying network traffic as recited in Claim 1, wherein the pattern includes a regular expression.

13. A method for identifying network traffic as recited in Claim 1, wherein the pattern includes application protocol information.

14. A method for identifying network traffic as recited in Claim 1, wherein the pattern
20 includes commonly used port information.

15. A method for identifying network traffic as recited in Claim 1, in the event the data does not match the pattern, further comprising returning a failure indicator.

16. A method for identifying network traffic as recited in Claim 1, wherein determining whether the pattern matching data matches the pattern occurs at the beginning of session.
17. A method for identifying network traffic as recited in Claim 1, wherein
5 comparing the pattern matching data with a pattern is performed for each received data.
18. A method for identifying network traffic as recited in Claim 1, further comprising comparing a second pattern matching data with a second pattern, wherein comparing the second pattern matching data occurs substantially concurrently with the comparing of pattern matching data with the pattern.
- 10 19. A method for identifying network traffic as recited in Claim 1, wherein comparing the pattern matching data with a pattern and determining whether the pattern matching data matches the pattern is performed using Boost Library.
20. A system for identifying network traffic comprising:
an interface configured to receive pattern matching data;
15 a processor configured to compare the pattern matching data with a pattern and determine whether the pattern matching data matches the pattern.
21. A computer program product for identifying network traffic, the computer program product being embodied in a computer readable medium and comprising computer instructions for:
20 receiving pattern matching data;
comparing the pattern matching data with a pattern; and
determining whether the pattern matching data matches the pattern.
22. A method for identifying network traffic comprising:

receiving pattern matching data;
comparing the pattern matching data with a pattern; and
determining whether the pattern matching data matches the pattern;
wherein the pattern matching data includes application data.